

MATH 4/51002  
Review of Cyclic Groups and Orders

We will need the following basic results on cyclic groups and orders of elements in finite groups in order to determine the structure of the multiplicative group of a finite field. See §3.5 of the text or the MATH 4/51001 notes (primarily pages 55–58 and 71–75) for proofs.

- A group  $G$  is said to be *cyclic* if  $G = \langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$  for some  $g \in G$ .
- If  $G$  is a cyclic group then every subgroup of  $G$  is cyclic.
- If  $G$  is a *cyclic* group of order  $n$ , then  $G$  has *exactly* one subgroup of order  $d$  for each positive divisor  $d$  of  $n$ .
- In a group  $H$ , the order of an element  $h$  is  $o(h) = |\langle h \rangle|$ . If  $o(h)$  is finite, then  $o(h)$  is the smallest positive integer  $n$  such that  $h^n = e$ .
- If  $G$  is a finite group of order  $n$  and  $g \in G$ , then  $o(g) \mid n$ , and so  $g^n = e$ .
- If  $G$  is a group and  $g \in G$  with  $o(g) = n$ , then  $o(g^m) = \frac{n}{(n,m)}$  for any integer  $m$ .
- If  $G = \langle g \rangle$  is a cyclic group of order  $n$ , then  $o(g^m) = n$  (and so  $g^m$  is a generator) if and only if  $(m, n) = 1$ .
- If  $G$  is a cyclic group of order  $n$ , then  $G$  has exactly  $\varphi(n)$  distinct elements of order  $n$ , hence  $\varphi(n)$  distinct generators, where  $\varphi$  is the Euler  $\varphi$ -function. [Recall that  $\varphi(n)$  is the number of integers  $k$  with  $1 \leq k \leq n$  and  $(k, n) = 1$ .]